Statistique sur la cyclicité de Modules de Drinfeld de rang 2

Statistics aboute the cyclicity of a Drinfeld Modules of rank 2

Mohamed-Saadbouh MOHAMED-AHMED [a]

[a] *Département de Mathématiques, Université du Maine, Avenue Olivier Messiaen, 72085 Le Mans Cedex 9.France*

Résumé

Soit Φ un $\mathbf{F}_q[T]$-module de Drinfeld de rang 2, sur un corps fini L, une extension de degré n d'un corps fini $\mathbf{F}_q$. On étudie la cyclicité de la structure de A-module induite par Φ sur L.

Pour citer cet article : Mohamed-saadbouh.Mohamed-Ahmed, C. R. Acad. Sci. Paris, Ser. I ... (...).

Abstract

Let Φ be a Drinfeld $\mathbf{F}_q[T]$-module of rank 2, over a finite field $L = \mathbf{F}_{q^n}$. We will study the cyclic property of the structure L^Φ. We will prove that the latter is cyclic only for trivial extensions of $\mathbf{F}_q$. *To cite this article: Mohamed-Saadbouh Mohamed-Ahmed , C. R. Acad. Sci. Paris, Ser. I ... (...).*

1 Introduction

let K a no empty global field of characteristic p (namely a rational functions field of one indeterminate over a finite field) together with a constant field, the finite field $\mathbf{F}_q$ with p^s elements. We fix one place of K, denoted by ∞, and call A the ring of regular elements away from the place ∞. Let L be a commutator

Email address: `mohamed-saadbouh.mohamed-ahmed@univ-lemans.fr` (Mohamed-Saadbouh MOHAMED-AHMED).

field of characteristic p, $\gamma : A \to L$ be a ring A-homomorphism. The kernel of this A-homomorphism is denoted by P. We put $m =[L,\ A/P]$, the extension degree of L over A/P, and $d = degP$. We denote by $L\{\tau\}$ the polynomial ring of τ, namely, the Ore polynomial ring, where τ is the Frobenius of $\mathbf{F}_q$ with the usual addition and where the product is given by the commutation rule : for every $\lambda \in L$, we have $\tau\lambda = \lambda^q\tau$. A Drinfeld A-module $\Phi : A \to L\{\tau\}$ is a non trivial ring homomorphism and a non trivial embedding of A into $L\{\tau\}$ different from γ. This homomorphism Φ, once defined, define an A-module structure over the A-field L, noted L^Φ, where the name of a Drinfeld A-module for a homomorphism Φ. This structure of A-module depends on Φ and, especially, on his rank. We will make a statistic, analogue to the statistic for elliptic curves by Vladut in[4], about the ordinary Drinfeld A-modules such that the A-modules L^Φ are cyclic, we note by $C(d, m, q)$ the proportion of the number (of isomorphisms of) ordinary Drinfeld A-modules, of rank 2 such that the A-modules structures L^Φ are cyclic, this means : if we note by $\#\{\Phi$, isomorphism, ordinary $\}$ the number of classes of L-isomorphisms of an ordinary Drinfeld Modules of rank 2, we have :

$C(d, m, q) = \frac{\#\{\Phi, L^\Phi cyclic\}}{\#\{\Phi, isomorphism, ordinary\}}$ and we note by $C_0(d, m, q)$ the proportion of the number (of isogeny classes of) ordinary Drinfeld A-modules, of rank 2 such that the A-modules L^Φ are cyclic, otherwise, if we note by $\#\{\Phi$, isogeny, ordinary$\}$ the number of isogeny classes, of ordinary Drinfeld modules of rank 2, we have : $C_0(d, m, q) = \frac{\#\{isogeny Classes of \Phi, L^\Phi cyclic\}}{\#\{\Phi, isogeny, ordinary\}}$, $C(d, m, q) = C_0(d, m, q) = 1$ if and only if $m = d = 1$.

This means that, to have a cyclic Drinfeld A-modules we must have a trivial extension L, and we let think, in conjecture form, that for a big q the values of $C(d, m, q)$ and $C_0(d, m, q)$ will tend to 1.

2 Cyclicity Statistics for the A-module $\mathbf{L}^\Phi$

We define $C(d, m, q)$ as been the ration of the number of (isomorphism classes of) Drinfeld modules of rank 2 with cyclic structure L^Φ to the number of L-isomorphisms classes of ordinary Drinfeld modules of rank 2, noted by $\#\{\Phi$, isomorphism, ordinary$\}$: $C(d, m, q) = \frac{\#\{\Phi, L^\Phi cyclic\}}{\#\{\Phi, isomorphism, ordinary\}}$, as same, we define $N(d, m, q)$ as been the ration of the number of (isogeny classes of) Drinfeld modules of rank 2 with not cyclic structure L^Φ to the number of L-isomorphisms isogeny of ordinary Drinfeld modules of rank 2, noted by $\#\{\Phi$, isogeny, ordinary$\}$: $N(d, m, q) = \frac{\#\{\Phi, L^\Phi noncyclic\}}{\#\{\Phi, isogeny, ordinary\}}$. We remark that : $0 \leq C(d, m, q), N(d, m, q) \leq 1$. J. Yu in [3], was proved that the charecteristic polynomial P_Φ of a Drinfeld module Φ can be given by : $P_\Phi(X) = X^2 - cX + \mu P^m$, such that $\mu \in \mathbf{F}_q^*$, and $c \in A$, where $\deg c \leq \frac{m.d}{2}$ by the Hasse-Weil analogue in this case.

Since the no cyclicity of the structure L^{Φ} needs the fact that $i^2 \mid P_{\Phi}(1)$ and $i_2 \mid (c-2)$, it is natural to introduce i (so i_2) in the calculus of $C(d,m,q)$ and $N(d,m,q)$. We fix the characteristic polynomial P_{Φ}, this means that we fix the isogeny classes of Φ, and we define :

Definition 2.1 *We note by* $n(P_{\Phi}, i_2) = \#\{\Phi : L^{\Phi} = \frac{A}{(i_1)} \oplus \frac{A}{(i_2)}\}$.

Remark 1 The number $n(P_{\Phi}, i_2)$ *is equal to the number of isomorphisms classes of* Φ *whole the A-module* $L^{\Phi} \simeq \frac{A}{(i_1)} \oplus \frac{A}{(i_2)}$*, in one isogeny classes, from where is coming the correspondence between* Φ *and* i_2*.*

For $n(P_{\Phi}, i_2)$ we have :

Lemma 2.2 *Let* $P_{\Phi}(X) = X^2 - cX + \mu P^m$ *be the characteristic polynomial of an ordinary Drinfeld A-module* Φ *of rank 2, and let* i_2 *be an unitary polynomial of A. Then if* $i_2 \mid c-2$ *we have :* $n(P_{\Phi}, i_2) \geq 1$*, else* $n(P_{\Phi}, i_2) = 0$*.*

We can deduct :

Corollary 2.3 *With the above notations :*

$$\#\{\Phi, L^{\Phi} noncyclic\} = \sum_{P_{\Phi}} \sum_{i_2, i_2^2 \mid P_{\Phi}(1)} n(P_{\Phi}, i_2).\#\{i_2, i_2^2 \mid P_{\Phi}(1) and i_2 \mid (c-2)\},$$

$$\#\{\Phi, L^{\Phi} cyclic\} = \sum_{P_{\Phi}} \sum_{i_2, i_2^2 \mid P_{\Phi}(1)} n(P_{\Phi}, i_2).\#\{i_2, i_2^2 \nmid P_{\Phi}(1) and i_2 \mid (c-2)\},$$

and if we note by $n_0(P_{\Phi}, i_2) = \#\{isogeny\ classes\ of\ \Phi : L^{\Phi} = \frac{A}{(i_1)} \oplus \frac{A}{(i_2)}\}$ *, we have :* $n_0(P_{\Phi}, i_2) = 1$*.*

We note now by $\#\{\Phi$, isogeny, ordinary $\}$ the number of isogeny classes, for an ordinary module Φ, then we define : $N_0(d,m,q) = \frac{\#\{isogeny classes of \Phi, L^{\Phi} not cyclic\}}{\#\{\Phi, isogeny, ordinary\}}$, the same for $C_0(d,m,q) = \frac{\#\{isogeny Classes of \Phi, L^{\Phi} cyclic\}}{\#\{\Phi, isogeny, ordinary\}}$,

We can so announce the following lemma :

Lemma 2.4 *With the notations above, we have :*

$$N_0(d,m,q) = \frac{\#\{i_2, i_2^2 \mid P_{\Phi}(1) and i_2 \mid (c-2)\}}{\#\{\Phi, isogeny, ordinary\}},$$

$$N(d,m,q) = \frac{\sum_{P_{\Phi}} \sum_{i_2, i_2^2 \mid P_{\Phi}(1)} n(\Phi, i_2).\#\{i_2, i_2^2 \mid P_{\Phi}(1) and i_2 \mid (c-2)\}}{\#\{\Phi, isomorphism, ordinary\}},$$

$C_0(d,m,q) = \frac{\#\{i_2, i_2^2 \nmid P_\Phi(1) et i_2 | (c-2)\}}{\#\{\Phi, isogeny, ordinary\}}$, $C(d,m,q) = \frac{\sum_{P_\Phi} \sum_{i_2, i_2^2 \nmid P_\Phi(1)} n(\Phi, i_2).\#\{i_2, i_2^2 \nmid P_\Phi(1) and i_2 | (c-2)\}}{\#\{\Phi, isomorphism, ordinary\}}$, *and* $N(d,m,q) + C(d,m,q) = 1,\ N_0(d,m,q) + C_0(d,m,q) = 1.$

The calculus of $\#\{\Phi$, isogeny, ordinary$\}$, for an ordinary A-module Φ, has been calculated in [1], as been :

Proposition 2.5 *Let $L = F_{q^n}$ and P the A-characteristic of L. We put $m = [L : A/P]$ and $d =$deg P :*

(1) m is odd and d is odd :$\#\{\Phi, isogeny, ordinary\} = (q-1)(q^{[\frac{m}{2}d]+1} - q^{[\frac{m-2}{2}d]+1} + 1)$.

(2) $m.d$ even : $\#\{\Phi, isogeny, ordinary\} = (q-1)(\frac{(q-1)}{2} q^{\frac{m}{2}d} - q^{\frac{m-2}{2}d} + 1)$.

As for the number L-isomorphisms classes, we will need the following result, for the proof and more details see [3] :

Proposition 2.6 *Let L be a finite extension of degree n over $\mathbf{F}_q$, then the number of L-isomorphisms classes of a Drinfeld A-module of rank 2 over L is $(q-1)q^n$ if n is odd and $q^{n+1} - q^n + q^2 - q$ else.*

And to calculate the number of L-isomorphisms classes for an ordinary Drinfeld modules, we will need to calculate the number of L-isomorphisms classes for a supersingular Drinfeld modules and subtract it from the global number of L-isomorphisms classes, for this, we have by [3] :

Proposition 2.7 *Let L be a finite extension of n degrees over $\mathbf{F}_q$, then the number of L-isomorphisms classes of a supersingular Drinfeld A-module of rank 2, over L is $(q^{n_2} - 1)$, where $n_2 =$ pgcd$(2, n)$.*

The calculus of $C(d,m,q)$ will be calculated in function of the values of d and m which are two major values to determinate c because deg $c \leq \frac{m.d}{2}$. And to calculate the number of L-isomorphisms classes existing in each isogeny classes, we need the following Definition for more information, see [4] :

Definition 2.8 *Let L be a finite extension of degree n over $\mathbf{F}_q$, we define $W(F)$ as been :*

$W(F) = \sum_{\Phi, F = Frobenius(\Phi, L)} Weigh(\Phi)$ *where :* $Weigh(\Phi) = \frac{q-1}{\#Aut_L \Phi}$.

$W(F)$ is the sum of weights(noted Weigh(Φ)) of number of L-isomorphisms classes existing in each isogeny classes of the module Φ which the Frobenius is F. And to calculate $\#\mathrm{Aut}_L\Phi$ we have the following lemma :

Lemma 2.9 *Let Φ be an ordinary Drinfeld A-module of rank* 2*, over a finite field $L = F_{q^n}$, then : $\#Aut_L\Phi = q - 1$.*

By the previous lemma, we can see that Weight $(\Phi) = \frac{q-1}{\#Aut_L\Phi} = 1$, that means :

Corollary 2.10 *In the case of ordinary Drinfeld modules of rank 2, $W(F)$ is the number of L-isomorphisms classes existing in each isogeny classes.*

Definition 2.11 *Let D be an imaginary discriminant and let l a polynomial for which the square is a divisor of D and let $h(\frac{D}{l^2})$ the number of classes of the order for which the discriminant is $\frac{D}{l^2}$. We define the number of classes of Hurwitz for an imaginary discriminant D, noted $H(D)$ by : $H(D) = \sum\limits_{l} \sum\limits_{l^2 \mid D} h(\frac{D}{l^2})$.*

Lemma 2.12 *If α is an integral element over A, for which $O = A[\alpha]$ is an A-order, then $disc(A[\alpha])$ is equal to the discriminant of the minimal polynomial of α.*

What is interesting for us is the calculus of the $\mathrm{disc}(A[F])$ and since $\mathrm{disc}(A[F]) = \mathrm{disc}(P_\Phi)$. To calculate the number of classes $W(F)$, we have the following result, for proof see [4].

Proposition 2.13 *Let L be a finite extension of degree n of a field F_q and F the Frobenius of L, then :*

$W(F) = H(disc(A[F]))$.

It remains for us to calculate $n(\Phi, i_2)$:

Lemma 2.14 *Let P_Φ be the characteristic polynomial of an ordinary Drinfeld A-module of rank* 2*, over a finite field L such that $L^\Phi = \frac{A}{(i_1)} \oplus \frac{A}{(i_2)}$, and let Δ the discriminant of the characteristic polynomial of the Frobenius F, then : $n(P_\Phi, i_2) = H(O(\Delta/i_2^2))$.*

3 Application

1) $d = m = 1$, in this case $L = A/P = \mathbf{F}_q$, the A-module $L^\Phi = A/P$ is cyclic, so $C(1, 1, q) = 1$. Conversely :

Theorem 3.1 *Let $L = F_{q^n}$ and P the A-characteristic of L, $m = [L, A/P]$ and $d = degP$. Then : $C_0(d, m, q) = C(d, m, q) = 1 \Leftrightarrow m = d = 1$.*

2)$m = 1$ et $d = 2$, In this case $n = m.d = 2$, and $n_2 = 2 \Rightarrow \#\{\Phi$, isomorphism, ordinary$\} = q^3 - q - (q^2 - 1) = q^3 - q^2 - q + 1$. $C_0(2,1,q) = \frac{q(q-1)-5}{q(q-1)-2}$,

$$C(2,1,q) = \frac{q^3-q^2-q+1-[\frac{q-1}{2}\sum_{P_\Phi}\sum_{i_2,\, i_2^2 | 4-4\mu P} H(O(\frac{4-4\mu P}{i_2^2}))+(q-1)\sum_{P_\Phi}\sum_{i_2, i_2^2 | c^2-4\mu P} H(O(\frac{c^2-4\mu P}{i_2^2}))]}{q^3-q^2-q+1}.$$

3)$m = 2$ and $d = 1$, in this case $n = m.d = 2$, and $n_2 = 2 \Rightarrow \#\{\Phi$, isomorphism, ordinary$\} = q^3 - q - (q^2 - 1) = q^3 - q^2 - q + 1$. $C_0(1,2,q) = \frac{(q-1)q-4}{(q-1)q-2}$,

$$C(1,2,q) = \frac{q^3-q^2-q+1-\sum_{P_\Phi}\sum_{i_2,\, i_2^2 | c^2-4\mu P} H(O(\frac{c^2-4\mu P}{i_2^2}))}{q^3-q^2-q+1}.$$

By the calculus of $C_0(d,m,q)$ and $C(d,m,q)$ for $m.d \leq 2$, we have : $\lim_{q\to\infty} C_0(1,1,q) = \lim_{q\to\infty} C_0(1,2,q) = \lim_{q\to\infty} C_0(2,1,q) = 1$, $\lim_{q\to\infty} C(1,1,q) = \lim_{q\to\infty} C(1,2,q) = \lim_{q\to\infty} C(2,1,q) = 1$. By the results above, we can give the following conjecture :

Conjecture 3.2 *Let $L = F_{q^n}$ and P the A-characteristic of L, $m = [L, A/P]$ and $d = degP$. Then :*

$$\lim_{q\to\infty} C(d,m,q) = \lim_{q\to\infty} C_0(d,m,q) = 1.$$

References

[1] M. S M. AHMED. Endomorphism Rings and Isogenies Classes for a Drinfeld A-Modules of Rank 2 over Finite Fields , preprint IML, 2004.

[2] David Goss. *Basic Structures of Function Field Arithmetic*, Volume 35 Ergbnise der Mathematik und ihrer Grenzgebiete, Springer.

[3] J-K. Yu. *Isogenis of Drinfeld Modules Over Finite Fields*. J. Number of Theory 54 (1995), no 1, 161–171.

[4] S.G. Vladut. *Cyclicity Statistics for Elliptic Curves Over Finite Fields*, Finite Fields Appl. 5 (1999), no 4, 354–363.